AMENDMENTS TO THE CLAIMS

Claims 1-3 (Cancelled)

4. (Original) A system for programmatic role-based security in a dynamically generated user interface, the system comprising:

an application framework configured through a deployment descriptor comprising a listing of a set of views, a listing of associated program logic and a listing of a set of authorized roles for selected ones of said views;

a first view listed in said deployment descriptor and comprising a linkage to a second view listed in said deployment descriptor; and,

access checking logic disposed in said first view and programmed to omit said linkage where a role of an end user accessing said first view is not authorized to access said second view according to said listing of said set of authorized roles in said deployment descriptor.

5. (Original) The system of claim 4, wherein said application framework comprises the Struts framework.

6. (Original) The system of claim 4, wherein said program logic comprises servlets and wherein said views comprise Java server pages (JSPs).

7. (Original) The system of claim 6, further comprising a custom tag disposed in said first view for invoking said access checking logic and for omitting said linkage responsive to said access checking logic.

8. (Currently Amended) A method for programmatic role-based security in a dynamically generated user interface, ~~the method~~ comprising ~~the steps of~~:

authenticating access to a rendering of a selected view based upon a role of an end user requesting access to said selected view;

processing said selected view to identify a method call to access checking logic;

comparing said role to a set of roles authorized to access a different view associated with said access checking logic; and[[,]]

selecting to dispose ~~disposing~~ a link to said different view in said rendering of said selected view conditional upon said role matches a role in said set of roles, wherein

said access checking logic disposed in said selected view and programmed to omit said link upon said role of said end user accessing said selected view is not authorized to access said different view.

9. (Previously Presented) The method of claim 8, wherein said step of authenticating comprises the step of comparing said role to a set of roles associated with said selected view to locate a match for said role.

10. (Currently Amended) The method of claim 9, wherein

said locating step comprises the step of parsing a deployment descriptor for an application framework hosting said selected view and said different view to identify said set of roles.

Claim 11 (Cancelled)

12. (Currently Amended) A machine readable storage having stored thereon a computer program for programmatic role-based security in a dynamically generated user interface, the computer program comprising a routine set of instructions which when executed by a machine cause the machine to perform ~~the steps of~~:

authenticating access to a rendering of a selected view based upon a role of an end user requesting access to said selected view;

processing said selected view to identify a method call to access checking logic;

comparing said role to a set of roles authorized to access a different view associated with said access checking logic; and[[,]]

selecting to dispose ~~disposing~~ a link to said different view in said rendering of said selected view conditional upon said role matches a role in said set of roles, wherein

said access checking logic disposed in said selected view and programmed to omit said link upon said role of said end user accessing said selected view is not authorized to access said different view.

13. (Previously Presented) The machine readable storage of claim 12, wherein said step of authenticating comprises the step of comparing said role to a set of roles associated with said selected view to locate a match for said role.

14. (Original) The machine readable storage of claim 13, wherein said locating step comprises the step of parsing a deployment descriptor for an application framework hosting said selected view and said different view to identify said set of roles.

15. (Original) The machine readable storage of claim 12, wherein said processing step comprises the step of invoking external access checking logic for a located server page tag referencing said access checking logic.

Claim 16 (Cancelled)

17. (Previously Presented) The system of claim 4, wherein said access checking logic is programmed to display said linkage where a role of the end user accessing said first view is authorized to access said second view.